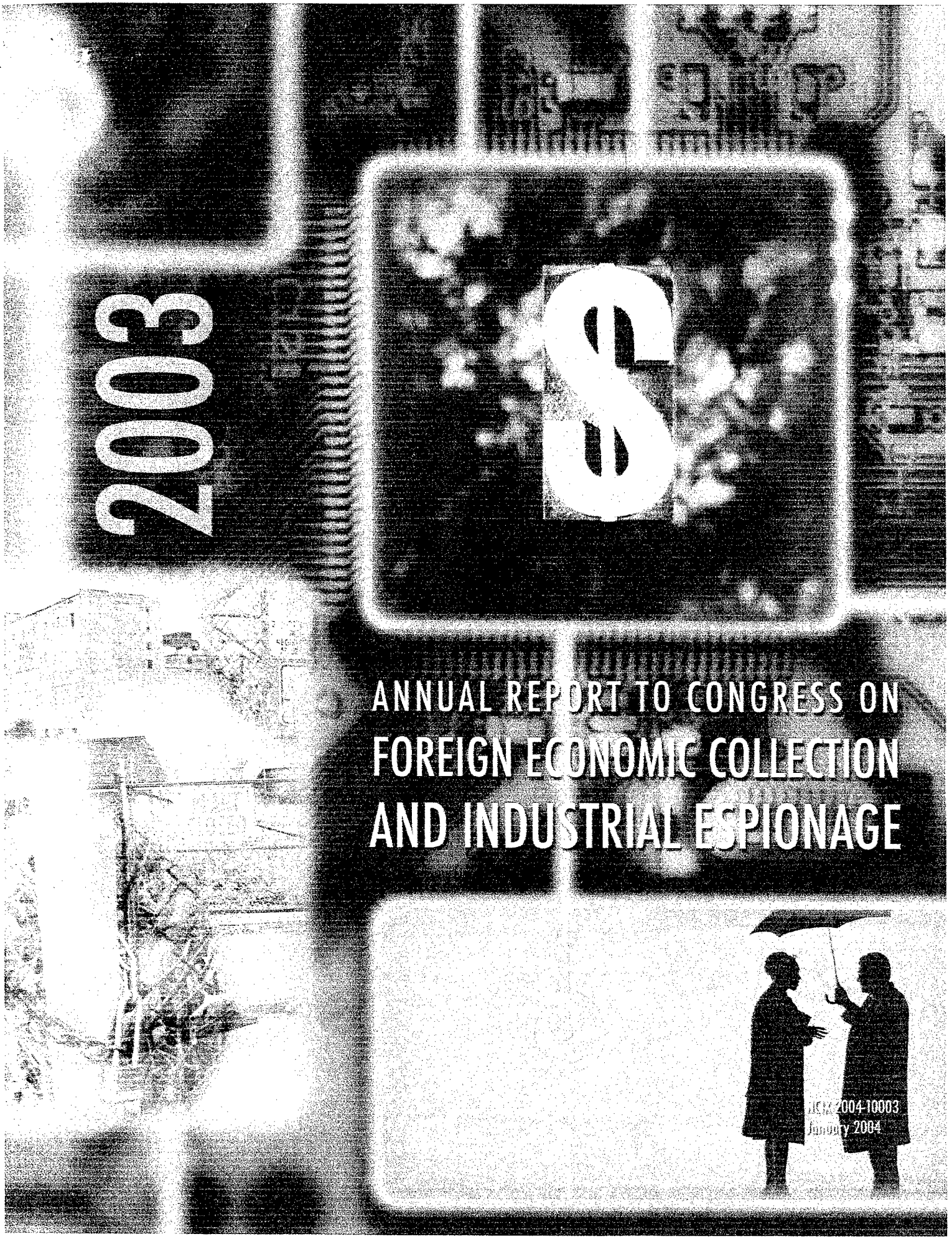


NCSC 2004-10003
January 2004


NATIONAL COUNTERINTELLIGENCE EXECUTIVE
UNITED STATES OF AMERICA

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2003

This report was prepared by the Office of the National Counterintelligence Executive. Comments and queries are welcome and may be directed to the National Counterintelligence Officer for Economics, ONCIX, on 703-874-8058. ONCIX may also be reached at www.ncix.gov.

Reverse Blank

NCIX 2004-10003
February 2004

INTENTIONALLY BLANK

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2003

Scope Note

This ninth annual report reviews the threat to the United States from foreign economic collection and industrial espionage. The report seeks to characterize and assess efforts by foreign entities—government and private—to unlawfully target or acquire critical US technologies, trade secrets, and sensitive financial or proprietary economic information. Although the title implies a heavy emphasis on technologies acquired for economic purposes, in reality it is difficult to determine the motives—military or commercial—of those targeting US technologies. Furthermore, sensitive US technologies initially acquired by foreign entities for military use frequently find their way into commercial application and vice versa. This paper makes no attempt to differentiate technologies acquired for civilian use from those acquired for military purposes. Instead, it focuses on all technologies, the loss of which could undermine US military superiority, impede the ability of the United States to compete in the world marketplace, and/or have an adverse effect on the US economy, eventually weakening national security.

The report is being submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809 (b), Public Law 103-359, which requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the eighth annual report published in February 2003. Unlike earlier reports that include data for only one year, this one includes information for calendar year 2002 and for January to September 2003. Data in the next annual report will be provided on a fiscal year basis (the tenth annual report will contain data for 1 October 2003 through 30 September 2004).

This assessment is a product of a cooperative effort across the entire Counterintelligence (CI) Community. It was compiled by the Office of the National Counterintelligence Executive (ONCIX) based on input from a broad cross-section of US Government entities. In particular, databases compiled by the Defense Security Service, the Air Force Office of Special Investigations, the Army Counterintelligence Center, and the Army Case Control Office were instrumental in providing much of the detail for this assessment. The Federal Bureau of Investigation—the lead investigative agency for enforcing economic espionage statutes—provided significant information on cases being investigated under the Economic Espionage Act of 1996. In addition, the Counterintelligence Field Activity added important data on foreign visitors to the United States. A host of other organizations within the CI Community also made major contributions to and/or have coordinated on this report, including:

- Central Intelligence Agency's Counterintelligence Center
- Defense Intelligence Agency
- Defense Threat Reduction Agency

- Department of Energy
- Department of Homeland Security, Immigration and Customs Enforcement
- Department of Justice
- Department of State, including the Bureau of Intelligence and Research and the Bureau of Diplomatic Security
- National Aeronautics and Space Administration
- National Reconnaissance Office
- National Security Agency
- Naval Criminal Investigative Service

Key Findings

Foreign businessmen, scientists, academics, and government officials from more than 90 countries continued targeting sensitive US technologies and corporate trade secrets in both 2002 and 2003,[1] according to a variety of reporting available to the US Counterintelligence (CI) Community. However, entities from a few key countries accounted for the bulk of attacks. US openness to foreign trade and investment and the country's commitment to global information sharing through academic and scientific exchange—tools that have served as engines for economic growth—unfortunately leave US technologies highly exposed to foreign exploitation. The losses associated with this illicit outflow of dual-use and military technologies are difficult to detect and even more difficult to quantify, but we believe the flow has eroded the US global military and economic advantage and has weakened the ability of US intelligence agencies to provide timely and accurate information to policymakers.

Foreign collectors employed a wide variety of techniques in their quest to circumvent US restrictions in the acquisition of sensitive technologies. Naturally, the simplest, safest, and least expensive methods were the ones most widely used. In a surprising number of cases, foreigners—often through middlemen—targeted sensitive US technologies simply by requesting them via e-mail, fax or telephone. Even vague requests that provided little end-user information sometimes yielded positive results. Other techniques used by foreign collectors included:

- Acquiring or forming joint ventures with US firms in order to cloud the issue of foreign ownership.
- Marketing foreign services and products to US high-tech firms as a means of gaining access to sensitive facilities and, potentially even more damaging, to information technology networks.
- Using cyber tools to extract sensitive US information and technology or to damage US providers of those goods.
- Sending officials, businessmen, and technical specialists to the United States to gather information.
- Attending academic and scientific conferences and trade shows in the United States or abroad. US scientists, underestimating the importance of the information they share during these sessions, may inadvertently provide proprietary, sensitive, or classified information, while exhibits and technical materials offer unique access to actual products.

---

[1] Information in this report covers calendar year 2002 and January through September 2003. Future Annual Reports will report data on a fiscal year basis, with the next report covering data from October 2003 through September 2004.

- Tapping US travelers abroad using foreigners trained to ask probing questions, monitoring hotel rooms or conference centers, or using unnecessary airport checks to search luggage or to download proprietary information from laptops.

- Applying variations of traditional espionage techniques of spotting, assessing, and recruiting.

The US technologies targeted in 2002 and 2003 were as diverse as the collectors and their tools. As in previous years, all 18 militarily critical technologies were targeted. Dual-use technologies—those that both support military force modernization and enhance commercial ventures—were, again, the most sought after items, according to a variety of intelligence reporting. Much of the information sought—more than 90 percent according to DSS calculations in 2003—was not classified, although it was export-controlled. Information systems technology attracted the most attention, while armaments and energetic materials and electronics were among the other militarily critical technologies in greatest demand. Foreign entities also sought a broad range of civilian technologies. Pharmaceuticals, biometrics, nanotech/miniaturization, manufacturing processes, and public safety systems exemplify the range of restricted or proprietary civilian technologies targeted.

The CI Community envisions no letup in the threat to US technologies over the next five years. Competitive economic and military pressures will force foreign entities to continue seeking state of the art US technology. Legal means of acquisition are likely to be employed first, but, if those fail, illicit transfer is the logical next step.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2003

The Nature of the US Industrial Espionage Problem

> *"You might as well sell this to us. We are going to get it anyway."*
>
> *FBI records quoting the US representative of a firm brokering technology transfer to a major foreign power.*

Foreign businessmen, scientists, academics, and government officials continued to aggressively target a variety of US technologies in 2002 and 2003. The attraction, and the primary reason foreigners willingly risked the penalties associated with the theft of US trade secrets and other proprietary information,[2] is obvious. The United States is now, and is likely to remain for the foreseeable future, the provenance of much of the world's most sophisticated science and technology. The US position at the top of the technology ladder is ensured by, inter alia, the deep capital markets that both finance and reward creative originality and the unparalleled university system that prizes innovative research and that attracts the best and brightest minds in the world.

Many foreign governments have come to believe that technology is the most important contributor to increasing their power relative to the United States and other nations. Similarly, businesses recognize that a technological lead can help assure growth in market share and profits. The temptation to acquire technology from the leader by illicit means is substantial for both governments and businesses and reflects a particular challenge for the United States. Strong global demand for US technology also creates a retail market into which middlemen—in search of profits—acquire US trade secrets for sale to the highest bidder. Global trading centers are frequently only stopover points for US technology illegally acquired for sale in other markets.

The openness of the US economy—a characteristic that has fostered our rapid economic growth—makes technology difficult to protect and vulnerable to theft. For example, US policy encourages foreign direct investment domestically, and our high-tech industries stay on the cutting edge, in part, by attracting both outside capital and innovative ideas. However, foreign investment also serves as a bridge, which foreigners use to circumvent export controls and to transfer abroad sensitive or controlled US technologies. The US university system—particularly technical sciences, which serve as the foundation for research and development—is another strength for the economy but also a vulnerability when it comes to safeguarding the flow of technology overseas. Many foreigners, who obtain scientific training in the best US universities, go on to work in US high-tech industries, and then eventually return with those skills and seek employment in competing firms in their home countries. US laws and regulations intended to restrict the flow of sensitive technologies—such as the Export Administration Act, the Economic Espionage Act, and export regulations—are often difficult to interpret and enforce in such a freewheeling environment.

Global connectivity via the Internet adds to US vulnerability. A variety of evidence suggests that foreign interests are increasingly looking to cyber tools as a means to illegally acquire trade secrets. Detection of such incursions is difficult, and no one is certain how much technology and sensitive proprietary information are lost annually to cyber theft. In addition, the Internet has given foreign interests an easy, inexpensive, and safe way to seek out firms and individuals who are willing to ignore or short-circuit export restrictions on sensitive US technologies.

[2] No other country in the world has laws specifically designed to punish the theft of commercial trade secrets. The US Economic Espionage Act of 1996 provides criminal penalties for individuals found guilty of stealing US trade secrets. Punishment is especially severe for theft done specifically to benefit foreign agents, whether or not the theft actually had foreign agent backing.

Useful Terms Related to Theft of Trade Secrets

Industrial Espionage: The theft of sensitive information that has independent economic value and that the owner has taken reasonable measures to protect, regardless of the perpetrator's country of origin or whether a foreign government agent can be linked to the theft. Sensitive information encompasses all types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, formulas, designs, prototypes, techniques, processes, programs, and codes, whether tangible or intangible and regardless of how the information is stored.

Economic Espionage: To avoid confusion, this report uses the term "economic espionage" sparingly and only when the description specifically fits the definition provided in Section 1831 of the Economic Espionage Act of 1996, i.e., the theft of trade secrets in which the perpetrator acts intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent.

Export Administration Regulations (EAR): Regulations issued by the US Department of Commerce, Bureau of Industry and Security and designed to restrict the export of US dual-use technologies (i.e., having both military and civil applications) to countries or persons that might apply such items to uses inimical to US interests. These regulations include controls designed to stem the proliferation of weapons of mass destruction and their delivery means, and controls designed to limit the military and terrorism support capability of certain countries. The regulations also include export controls to protect the United States from the adverse impact of the unrestricted export of commodities in short supply.

International Trade in Arms Regulations (ITAR): The US law—also called Defense Trade Regulations—that governs the export of US arms and implements of war (including cryptography) and defense technology. ITAR, which is administered by State Department's Office of Defense Trade Controls, allows the US Government to deny export licenses and agreements to proscribed countries that could misuse or cause illegal proliferation of those items.

The Counterintelligence (CI) Community cannot accurately establish the dollar cost to the nation of the loss of trade secrets, but we believe the flow has eroded the US global military and economic advantage. One of the challenges that makes calculating the cost of industrial espionage particularly difficult is that the losses often are not readily apparent. The only indication a US company may have that its research and development plans or its marketing strategies have been stolen is a shrinking market share as foreign and domestic firms take advantage of price and product information to steal customers. Likewise for national security secrets, often the only evidence of a loss of a key military technology is the emergence of a new or more sophisticated weapon or countermeasure in a foreign arsenal years later.

When trade secret theft is detected, it is not always prosecuted. Political, foreign policy, and CI concerns, as well as prosecutorial discretion, sometimes override willingness to prosecute. Then too, a US company—fearful of how its stockholders might react to news that it has been subject to industrial espionage—may simply ignore the incursion. The unwillingness to prosecute lowers the risk to foreigners considering illegal acquisition of US trade secrets and thereby facilitates theft.

The Sponsors of Industrial Espionage

Foreigners from almost 90 countries attempted to acquire sensitive technologies from the United States

in 2003, according to data compiled from across the CI Community, about the same number as in 2002. While foreign government officials were behind some of the incidents, they by no means accounted for the majority of collection attempts. For example, Defense Security Service (DSS) data show that only about 15 percent of suspicious efforts to illegally acquire sensitive US military-related technology in 2003 directly involved foreign governments. Another 25 percent came from government-affiliated organizations or foreign companies that work solely or predominantly for foreign governments, according to DSS statistics. The remainder came from individuals (14 percent) claiming to be working for themselves and from company representatives (31 percent); in 15 percent of cases, there was no indication of affiliation (see figure 1).

The large number of countries involved is an indication of the extent of the industrial espionage problem, [3] but it would be inaccurate to classify the majority of these countries as major players in this game. In fact, most are not now, nor ever have been, aggressive collectors against the United States. Instead, a relatively few key countries consistently account for the lion's share of all collection activity against the United States.

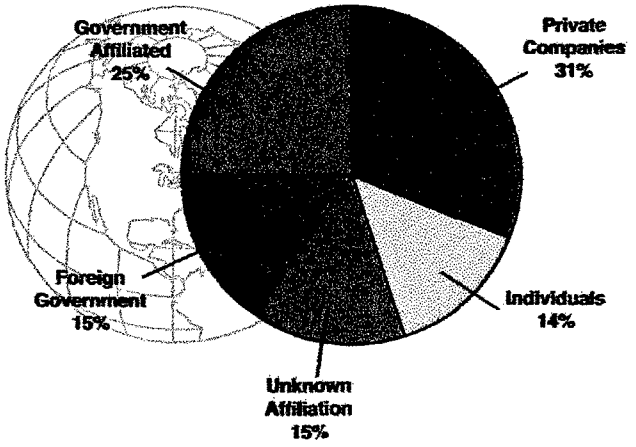
Techniques for Stealing Trade Secrets

The tools and techniques for acquiring sensitive US technologies have evolved over time to take advantage of increased access. Not surprisingly, the most widely used techniques are also the simplest, safest, and least expensive.

In a number of cases, foreigners have acquired sensitive US technologies simply by asking for them. Foreign entities request access to sensitive information or technologies using e-mail, faxes, or telephones. The ease and risk-free nature of these techniques explain their widespread application. DSS and the Air Force Office of Special Investigations (AFOSI) break these requests into two categories: "requests for information" and "attempted acquisitions." A **request for information (RFI)** is any request, not sought or encouraged by the cleared company, received from a

[3] Another measure of the extent of the problem is the number of prosecutions for the illegal export of US technology. During fiscal year 2003, US Department of Immigrations and Customs Enforcement (ICE) conducted more than 2000 investigations involving violations of the Arms Export Control Act, International Traffic in Arms Regulations, Export Administration Regulations, International Emergency Economic Powers Act and the Trading with the Enemy Act. Those investigations resulted in 120 arrests, 75 criminal indictments and 55 convictions during FY 2003.

Figure 1: (U) Types of Foreign Collectors Targeting US Militarily Critical Technologies, 2003* (percent of suspicious incidents)



* Based on DSS reporting

known or unknown source that concerns classified, sensitive, or export-controlled information. The fact that the solicitor has little reason to know about the technology, by itself, is sufficient to make US contractors suspicious of the inquiry. Such requests are often more probing exercises than actual attempts to acquire the goods. Those making the inquiries often provide few specific details on product requirements and even less end-user information.

Attempted acquisitions, on the other hand, tend to be more specific, providing technical details about the sensitive products being sought and requesting pricing information. On occasion, these acquisition attempts involve foreign entities attempting to gain access to sensitive technologies by purchasing US companies. Attempted acquisitions often bypass the usual marketing offices and go, instead, to an individual inside the company, which heightens the concerns of the cleared contractors who report this activity.

Such inquiries, in and of themselves, are not illegal. US firms that respond by requiring end-user information or by pointing out that export licenses will be needed before the technology can be delivered are simply ignored. Thus, the vast majority of these direct requests yield no positive results. Given the almost cost-free nature of this technique, however, the search simply continues until a supplier is located that, for the right price, will dispense with or circumvent legal prohibitions and export the restricted technology abroad. The short-term profits go, unfortunately, to the US firms most willing to bend or break the rules.

Often those making the requests are operating on behalf of unidentified end users. Sometimes the requesters operate out of front companies,[4] making it even more difficult to determine the true end users. Several different collectors may initiate nearly identical inquiries over a period of a few months. The US CI Community believes this indicates that a single end user hopes to increase the chance of success by going through multiple channels for a controlled technology. Each collector may approach several potential suppliers.

Sometimes requests to potential suppliers fail to identify a final destination for the product. Other times a collector will falsely identify an end user. When the true end user is a less developed country that lacks the means to make large purchases, a collector may misleadingly identify the end user as a large country in an effort to dangle high-volume, high-profit prospects in front of the seller. This sometimes results in less than perfect attention by the seller to such details as verifying the bona fides of the recipient and adhering strictly to US export-control laws. By establishing offices in the United States, foreign collectors sometimes take possession of sensitive goods ostensibly for domestic use. Later, the technology is smuggled out of the country.

Another collection technique favored for accessing sensitive US technologies in 2002 and 2003 was the **marketing of foreign services and products** to US high-tech firms. Foreign individuals with technical backgrounds offer their services to US research facilities, academic institutions, and even cleared defense contractors. This tool has been a favorite of foreign firms with hardware and software expertise. Installing and servicing their products in US companies gives these foreign firms access to both facilities and technologies that might not otherwise be available. Temporary access to information technology networks has the potential to turn into long-term entrée if the foreign firms are able to install Trojan horses or backdoors into sensitive computer networks. The beauty of this approach is that foreign firms are invited in and actually paid for providing a service while, at the same time, gaining access to technologies that might not otherwise be available to them.

Another collection method with great potential is the **exploitation of existing relationships with US firms**. Foreign offers to establish joint ventures or cooperative agreements in the United States with US firms made up the bulk of these efforts in 2002 and 2003, according to DSS and AFOSI reporting. Also of

[4] Front companies are firms that conduct business without revealing the individuals or motives behind the acquisition. Often such firms generate most of their revenue doing legitimate business. These firms play an important role in the illegal transfer of sensitive technologies abroad.

growing concern, however, is the increased reliance of US firms on foreign research facilities and software development companies to work on commercial projects that are related to protected programs. By relinquishing direct control of processes or products to foreign firms, US companies increase the likelihood of foreign exploitation.

The gains from this approach can be significant:

In forming joint ventures in the United States, foreign companies become US firms under the law. While such partnerships do not reduce or remove the restriction against exporting US technology abroad, the blending of ownership provides more opportunities for transfers to go undetected and makes it more difficult for enforcement agencies to monitor exports, especially violations of the "deemed export" prohibition.[5]

- Partnerships also make US technology more vulnerable by increasing foreign access to facilities and supply chains. Operational security practices inside firms are more difficult to enforce, for example, when the foreigner seeking access to a secure facility is a member of the management team.

- Cooperative agreements and joint ventures, particularly with US firms that handle sensitive US Government contracts, sometimes allow foreign firms to embed employees within US firms. This process can increase the threat to US technology if required safeguards are not in place and monitored on a frequent basis.

In 2002 and 2003, collectors also continued to employ the **Internet** in their efforts to access sensitive US technologies. Cyber tools were used to extract sensitive US information and technology, as well as to hack, scan, ping, or damage US providers of those goods.

Exploiting **foreign visits** to the United States is another potentially fruitful tool for those seeking US technology. Foreign visitors include those in the United States on a one-time basis, those who regularly travel back and forth, as well as long-term visitors (such as exchange employees, official government representatives, and students). No other country in the world offers its technological expertise so freely to foreign nationals because of the strong belief that the advantage from sharing technology and expertise is mutual. There were more than 100,000 "official" visits paid to DoD entities in the United States during the 18 months from January 2002 through June 2003, according to data provided by the Counterintelligence Field Activity. When these figures are added to the hundreds of thousands of foreigners studying in US universities or visiting, working, or training in US high-tech firms, the potential for technology loss is staggering (see figure 2 on page 6).

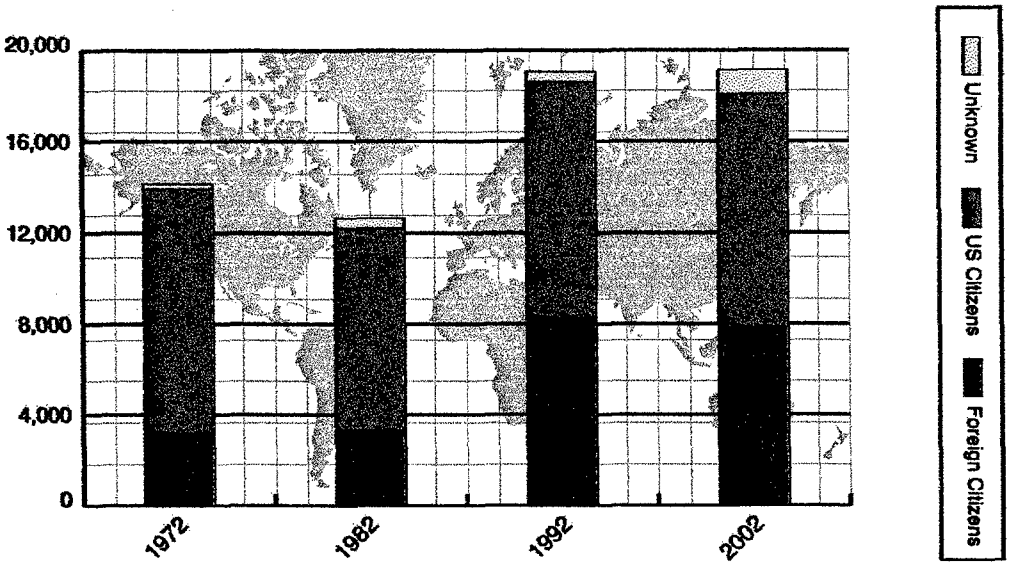
Many of these visitors have worked with sensitive technologies before coming to the United States and are well positioned to use their US visits to hone in on specific home-country technological gaps. In 2003 alone, more than 15,000 applications were reviewed under the Visa Mantis program, meaning they were slated to work with sensitive items that have been placed on the "technology alert list" maintained by the Department of State.[6] Besides their value in giving foreign experts immediate access to US trade secrets, visits to the United States are also used to spot and assess scientists, academics, and businessmen who might be willing to develop a long-term relationship that could lead to future opportunities to acquire sensitive items. Standard operational security procedures—such as not allowing photographs, enforcing strict escort rules, and forbidding unauthorized contact with US staff—undoubtedly limit the amount of technology lost to these visitors, but the continued frequency of the visits is a clear indication that both sides see them as highly beneficial.

Some of the suspicious technology acquisition incidents that took place in 2002 and 2003 occurred at academic and scientific **conferences and trade shows**. The audiences at international seminars are comprised principally of the leading national scientists and technical experts, who can pose more of a threat than intelligence officers. Technical experts focus their questions and requests on specific

[5] Under the Export Administration Regulations (EAR), an export of technology or source code (except encryption source code) is "deemed" to take place when it is released in any way, even verbally, to a foreign national within the United States.

[6] The "technology alert list" contains US technologies whose acquisition by a foreign government could be deleterious to US security.

Figure 2: (U) US Doctoral Recipients in Technical Sciences and Engineering



technical areas that have direct application to their work. Unsuspecting scientists can be easy targets of opportunity because they underestimate the importance of the information they share during these sessions—letting their guard down when talking to peers on arcane technical subjects—and inadvertently provide proprietary, sensitive, or classified information. Also, exhibits and technical materials available at the conferences offer a unique opportunity for foreign entities to study, compare, and photograph actual products in one location. Of even more importance, foreign events held on the collector's home territory are vulnerable to exploitation by traditional technical means (for example, electronic surveillance) and by the use of entrapment ploys, such as inducing targets into compromising situations.

US travelers abroad have traditionally been yet another important source of information on sensitive US technologies, and the last two years were no different. The free flow of information in the United States and the willingness of US scientists and scholars to engage in academic exchange make US travelers particularly vulnerable not only to standard electronic monitoring devices—installed in hotel rooms or conference centers—but also to simple approaches by foreigners trained to ask the right questions. Targeting occurs at airports and includes luggage searches, unnecessary inspection and downloading of information from laptop computers, and extensive questioning beyond normal security measures. Other travelers have received excessively "helpful" service by host government representatives and hotel staffs.

Variations of **traditional espionage techniques** of spotting, assessing, and recruiting are also occasionally practiced in industrial espionage.

The Most Sought After Technologies

As in the previous three years, foreign collectors in 2002 and 2003 targeted all 18 militarily critical technologies (MCTs).[7] Dual-use technologies—those that support military force modernization as well as

[7] The Militarily Critical Technologies List (MCTL) is a detailed compendium of information on technologies that the Department of Defense assesses are critical to maintaining superior US military capabilities. The acquisition of any of these technologies by a potential adversary would lead to the significant enhancement of the military-industrial capabilities of that adversary to the detriment of US security interests. See the 2002 Annual Report for a detailed breakdown of the items on the MCTL.

enhance commercial ventures—were, again, the most sought after of the militarily critical items during the calendar year, according to a variety of intelligence reporting. The majority of defense technologies targeted were components rather than complete systems, because the latter are subject to tighter scrutiny in the United States, are more expensive to acquire, and are more difficult to bring into production in most developing countries. In addition, most of the targeted technology was unclassified. According to DSS data, some 92 percent of the technology targeted by foreign collectors in 2003 was unclassified, up from 88 percent in 2002, although much of it was controlled under either the International Traffic in Arms Regulations (ITAR) administered by the Department of State or the Export Administration Regulations (EAR) administered by the Department of Commerce.

Among the sensitive MCTs targeted by foreigners in 2003, according to DSS data, (see table), information systems attracted the most attention, having been sought by more than 60 countries and accounting for one-fifth of all suspicious incidents. Sensors and lasers were second, with entities from 46 countries attempting purchases in 2003 and accounting for 17 percent of suspicious incidents. Also in high demand were armaments and energetic materials (44 countries, 9 percent of suspicious incidents) and electronics (32 countries and 9 percent of suspicious incidents).

Table 1: (U) The 10 Most Highly Targeted US Militarily Critical Technologies, 2002-2003, Based on DSS Data (Reported to DSS by cleared defense contractors)

Militarily Critical Technology	Number of Countries Targeting		Percent of Reported Suspicious Incidents	
	2003	2002	2003	2002
Information Systems	63	47	22	25
Sensors and Lasers	46	40	17	17
Electronics	32	37	9	12
Armaments and Energetic Materials	44	26	9	9
Aeronautics	35	36	10	9
Marine Systems	34	24	4	6
Guidance and Navigation and Vehicle Control	25	15	4	4
Space Systems Technologies	19	22	5	3
Power Systems	13	13	2	3
Manufacturing and Fabrications	21	16	3	3

Pharmaceuticals, biometrics, nanotech/miniaturization, manufacturing processes, public safety systems, and patent rights exemplify the range of restricted or proprietary civilian technologies that foreign entities target. Computer technologies, biotechnology, and public security technologies (identity recognition, bomb detection, and emergency response) were of particular interest in 2002 and 2003. For example, foreign collectors highly valued advanced computer chip technologies, such as proprietary and export-restricted processors, semiconductors, and circuitry. Finally, foreign entities also targeted diverse assets of the energy, agriculture, automotive, machining, and environmental sectors.

The Road Ahead

There is every indication on both the domestic and global front that the already significant foreign threat to US technology will only increase over the next five years. Demand for dual-use technologies with military applications is also unlikely to taper off. Historical experience demonstrates that, whenever global or regional threats increase, there is a surge in efforts to acquire US military technology. As long as global or regional tensions are high, so too will be demand for sophisticated military and dual-use US technologies.

While forecasting a rise in foreign industrial espionage is straightforward, it is more difficult to predict exactly which technologies will be in greatest demand. Broadly speaking, of the militarily critical technologies, it is safe to say that information systems (IS) will remain in first place in terms of foreign demand. Even when new technological developments in that industry slowed, demand for the technology remained high as additional military and civilian applications of IS were discovered. Because electronics and sensors and lasers continue to be building blocks for much of the civilian and military sectors, they too will remain in high demand. CI analysts will closely monitor future foreign targeting efforts to determine which other specific technologies will be in greatest demand.